*Mr. drs. B. van der Sloot**

De nieuwe consumentenrechten in de Algemene verordening gegevensbescherming: vergeten worden, dataportabiliteit en profilering

De Europese Dataprotectierichtlijn stelt regels ten aanzien van de verwerking van persoonsgegevens. Anders dan het recht op privacy ziet het gegevensbeschermingsrecht niet zozeer op restricties, maar op waarborgen door middel van de codificatie van algemene zorgvuldigheidsnormen, en niet op de relatie tussen staat en burger, maar op die tussen burgers en bedrijven onderling. In januari 2012 is er een voorstel gedaan voor een Algemene verordening gegevensbescherming, die de richtlijn uit 1995 op termijn zal moeten vervangen. De verordening speelt onder meer in op het digitale tijdperk en de snelgroeiende internetdiensten. De verordening zet daarbij in op een vergroting van de handhavende rol van de staat en op concrete rechten van de consument, zoals het recht om vergeten te worden, het recht op dataportabiliteit en het recht op bescherming tegen profilering. Dit artikel belicht de belangrijkste wijzigingen onder de verordening, analyseert de nieuw toegekende consumentenrechten en beoordeelt in hoeverre de verordening consumenten in het digitale tijdperk een adequate bescherming zal bieden.

1. Introductie[1]

De Nederlandse Wet bescherming persoonsgegevens (Wbp), in werking getreden op 1 september 2001,[2] vormt de implementatie van de Europese Dataprotectierichtlijn,[3] die de verwerking van persoonsgegevens reguleert. In januari 2012 is er door de Europese Commissie een voorstel gedaan voor een Algemene verordening gegevensbescherming[4] die de Dataprotectierichtlijn uit 1995 op termijn zal moeten vervangen. Een dergelijke algehele herziening van de dataprotectieregels werd al langer wenselijk geacht gezien de sterke opkomst van internetgerelateerde diensten en applicaties. Dit artikel beschrijft in welke mate consumenten, of in dataprotectietermen 'datasubjecten', onder de nieuwe verordening beter worden beschermd. Daarbij wordt met name stilgestaan bij drie (gedeeltelijk) nieuwe rechten die aan de consument worden toegekend: het recht om vergeten te worden zal worden beschreven in paragraaf 3, het recht op dataportabiliteit zal worden uiteengezet in paragraaf 4 en de bescherming tegen profilering zal worden besproken in paragraaf 5. Daarna zal worden geanalyseerd in hoeverre de nieuwe verordening een effectieve bescherming van het gegevensbeschermingsrecht zal bewerkstelligen in een wereld waarin elektronische ontwikkelingen elkaar snel opvolgen. Eerst worden in de introductie nog een aantal algemene begrippen uit het huidige dataprotectierecht vermeld en in paragraaf 2 wordt kort uit de doeken gedaan welke algemene wijzigingen er in de nieuwe verordening worden voorgesteld.

Het recht op gegevensbescherming is gelieerd aan, maar wordt desalniettemin in toenemende mate onderscheiden van het recht op privacy. Zo maakt het Handvest van de grondrechten van de Europese Unie uit 2000, in tegenstelling tot het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM), een onderscheid tussen artikel 7, dat stelt dat eenieder recht heeft op eerbiediging van zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn communicatie, en artikel 8, dat stelt dat eenieder het recht heeft op bescherming van de hem betreffende persoonsgegevens, dat deze gegevens eerlijk en voor bepaalde doeleinden moeten worden verwerkt op basis van een legitieme verwerkingsgrondslag en dat het datasubject het recht op rectificatie heeft.[5] Het recht op privacy wordt over het algemeen beschouwd als een recht met een morele connotatie, dat ziet op de bescherming van de autonomie,[6] waardigheid[7] en persoonlijke vrijheid[8] van een individu, terwijl dataprotectie zich voornamelijk richt op de zorg-

* Onderzoeker aan het Instituut voor Informatierecht (IViR) van de UvA

1. Het onderzoek voor dit artikel is op 24 augustus afgerond; wijzigingen, ontwikkelingen en discussies van na die datum zijn derhalve niet meegenomen in dit stuk.
2. *Kamerstukken II* 1997/98, 25 892, *Stb.* 2000, 302 en *Stb.* 2001, 337.
3. Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (Dataprotectierichtlijn).
4. http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_nl.pdf.
5. Handvest van de grondrechten van de Europese Unie (*PbEG* 2000, C 364/01), www.europarl.europa.eu/charter/pdf/text_nl.pdf.
6. B. Roessler, *The value of privacy*, Cambridge: Polity Press 2005; A.F. Westin, *Privacy and Freedom*, London: The Bodley Head 1970.
7. Zie o.a.: S.I. Benn, 'Privacy, Freedom, and Respect for Persons', in: F. Schoeman (red.), *Philosophical Dimensions of Privacy: an Anthology*, Cambridge: Cambridge University Press 1984, p. 223-244; J.Q. Whitman, 'The Two Western Cultures of Privacy: Dignity Versus Liberty', *The Yale Law Journal* 2004, 113.
8. Zie o.a.: J.S. Mill, *On liberty*, New York: Norton 1975.

vuldige en rechtmatige verwerking van persoonsgegevens.[9] Terwijl privacy van oudsher een afweerrecht is van de burger tegen de staat,[10] legt het dataprotectierecht slechts in beperkte mate restricties op en ziet het primair op horizontale relaties, dat wil zeggen tussen burgers of bedrijven onderling.[11]

Een ander verschil is dat een persoonsgegeven, een kernbegrip uit het dataprotectierecht, niet het privéleven van een persoon hoeft te betreffen, maar wordt gedefinieerd als iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.[12] Zo kan bijvoorbeeld de zinsnede 'De man in de zwarte jas bij de lantaarnpaal' een persoonsgegeven zijn,[13] waardoor de vereisten uit de Dataprotectierichtlijn van toepassing zijn op de 'verwerking' van dit gegeven; 'verwerken', een tweede kernbegrip uit de richtlijn, is praktisch alles wat er met gegevens kan worden gedaan, zoals het opslaan, verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, gebruiken, verstrekken, verspreiden, afschermen, uitwissen of vernietigen van gegevens.[14]

Eén pilaar van het dataprotectierecht wordt gevormd door de zogenoemde dataminimalisatieregels, die globaal inhouden dat er zo min mogelijk persoonsgegevens mogen worden verzameld, dat deze in verhouding moeten zijn met het van tevoren nauwkeurig omschreven doel voor de verwerking, dat ze niet verder mogen worden verwerkt voor een ander doel dan waarvoor zij zijn verzameld en dat ze zo snel mogelijk moeten worden gewist als ze niet langer noodzakelijk zijn voor het bereiken van dit doel.[15]

De tweede en grotere pilaar wordt gevormd door de nadruk op de rechtmatigheid en de zorgvuldigheid van de gegevensverwerking. Zo bepaalt de richtlijn dat persoonsgegevens eerlijk en rechtmatig moeten worden verwerkt,[16] dat de data nauwkeurig en correct moeten zijn[17] en dat ze op een technisch veilige en zorgvuldige wijze moeten worden verwerkt, zonder gevaar op datalekken of onbevoegde toegang door derden.[18] Ook moet er informatie worden verstrekt door de verantwoordelijke voor de gegevensverwerking (kortweg: de verantwoordelijke) aan het datasubject zoals die betreffende zijn identiteit, de doeleinden van de verwerking en de ontvangers van de gegevens.[19] Daarnaast heeft het datasubject het recht dergelijke informatie van de verantwoordelijke te vragen en zich in bepaalde gevallen te verzetten tegen de verwerking van zijn persoonsgegevens.[20]

Deze principes zien derhalve niet zozeer op een beperking van of restricties op de verwerking van persoonsgegevens, maar bevatten vooral waarborgen voor een zorgvuldig en inzichtelijk gegevensverwerkingsproces.[21] Een laatste belangrijke waarborg die de richtlijn biedt is dat de verwerking van persoonsgegevens dient te geschieden op basis van één van de in de richtlijn opgesomde legitieme verwerkingsgrondslagen, zoals de toestemming van het datasubject, een contractuele of wettelijke verplichting of indien de belangen van de verantwoordelijke zwaarder wegen dan die van het datasubject.[22] Voor het verwerken van bijzondere persoonsgegevens, zoals gegevens betreffende ras, politieke of religieuze opvatting, gezondheid en seksuele voorkeur bestaan zwaardere eisen; zo geldt niet als legitieme verwerkingsgrondslag de afweging tussen de belangen van het datasubject en die van de verantwoordelijke.[23]

Tot slot is er in de richtlijn een zeer kleine rol weggelegd voor de handhavende autoriteit, in Nederland het College bescherming persoonsgegevens (CBP),[24] daarmee benadrukkend dat het dataprotectierecht zich primair richt op horizontale verhoudingen, waarbij de staat en de handhavende organisaties een teruggetrokken rol dienen te spelen. De handhaving van de regels uit de richtlijn geschiedt primair op nationaal niveau, op basis van de nationale, wettelijke implementatie van de richtlijn, en lidstaten genieten een ruime vrijheid ten aanzien van het stellen van regels met betrekking tot mogelijkheden voor beroep, aansprakelijkheid en sancties en boetes;[25] in Nederland is hier echter slechts marginaal invulling aan gegeven.[26] Er is een plicht voor bedrijven om gegevensverwerkingen te melden bij het CBP[27] en er bestaat de mogelijkheid voor specifieke branches om gedragscodes bij het CBP neer te leggen.[28] Beide verplichtingen spelen in

9. P.H. Blok, *Het recht op privacy: een onderzoek naar de betekenis van het begrip 'privacy' in het Nederlandse en Amerikaanse recht*, Den Haag: Boom Juridische uitgevers 2002.
10. Meer specifiek de plicht van de staat niet ongeoorloofd in het privéleven van burgers te treden, http://repository.ubn.ru.nl/bitstream/2066/15362/1/15362.pdf.
11. Zie o.a. artikel 3 en 13 Dataprotectierichtlijn.
12. Artikel 2 onder a Dataprotectierichtlijn.
13. Artikel 29-werkgroep, *Advies 4/2007 over het begrip persoonsgegeven*, 01248/07/NL, Brussel, 20 juni 2007.
14. Artikel 2 onder b Dataprotectierichtlijn.
15. Artikel 6 Dataprotectierichtlijn. Zie ook overweging 26 Dataprotectierichtlijn.
16. Artikel 6 onder a Dataprotectierichtlijn.
17. Artikel 6 onder d Dataprotectierichtlijn.
18. Artikel 16 en 17 Dataprotectierichtlijn.
19. Artikel 10 en 11 Dataprotectierichtlijn.
20. Artikel 12 en 14 Dataprotectierichtlijn.
21. Sterker nog, het vereiste om gegevens correct, nauwkeurig en up to date te houden en het recht op inzage kunnen met zich meebrengen dat er meer, niet minder gegevens moeten worden verzameld en opgeslagen.
22. Artikel 7 Dataprotectierichtlijn.
23. Artikel 8 Dataprotectierichtlijn.
24. Artikel 28 Dataprotectierichtlijn.
25. Artikel 22-24 Dataprotectierichtlijn.
26. Zie bijvoorbeeld artikel 66 Wbp.
27. Artikel 18-21 Dataprotectierichtlijn.
28. Artikel 27 Dataprotectierichtlijn.

de praktijk echter een zeer marginale rol.[29] Bedrijven worden aangemoedigd om zelf een functionaris voor de gegevensbescherming aan te stellen, die intern oog houdt op de conformiteit binnen het bedrijf met de richtlijn, maar dit betreft geen plicht.[30] Tot slot hebben alle 'CBP's' van Europa zich verenigd in een adviesorgaan,[31] de Artikel 29-werkgroep genaamd, dat niet bindende adviezen opstelt over specifieke onderwerpen.

2. Algemene uitgangspunten van de verordening

Wat ten eerste opvalt aan de voorgestelde verordening is haar omvang; terwijl de richtlijn 34 artikelen bevat, telt de verordening er 91. Een achterliggende reden hiervoor is dat er deels voor is gekozen om de nadruk op de algemene zorgvuldigheidsprincipes te verlaten en te kiezen voor meer concrete en toegepaste rechten en plichten.[32] Dit ondervangt één van de grootste kritiekpunten op de richtlijn, namelijk haar omnibuskarakter en het gebruik van open normen die in de praktijk als vaag en onduidelijk worden ervaren en weinig houvast bieden bij concrete vraagstukken en dilemma's.[33] Daarnaast zijn er nog een aantal belangrijke wijzigingen op te merken.

Zo is de laatste jaren veel te doen geweest omtrent de verwerkingsgrondslag die is gebaseerd op de toestemming van het datasubject, gedefinieerd als elke vrije, specifieke en op informatie berustende wilsuiting.[34] De vraag is bijvoorbeeld of toestemming in bepaalde gevallen ook op een generieke wijze mag geschieden en of een opt-outsysteem, waarbij er persoonsgegevens worden verwerkt tenzij iemand aangeeft hier bezwaar tegen te maken, afdoende is om als toestemming onder de richtlijn te kwalificeren. In de definitie van toestemming onder de verordening is thans toegevoegd dat deze 'uitdrukkelijk' moet zijn,[35] wat een opt-outsysteem lijkt uit te sluiten.[36] Daarbij specificeert een afzonderlijk artikel, dat indien dit als de legitieme verwerkingsgrondslag door de verantwoordelijke wordt aangemerkt, hij moet kunnen aantonen dat de betrokkene toestemming heeft gegeven voor de verwerking, wat derhalve een omkering van de bewijslast met zich meebrengt, dat toestemming niet mag zijn gegeven in het kader van een andere aangelegenheid dan van de verwerking, dat de betrokkene het recht heeft om zijn toestemming in te trekken en dat de toestemming van een hiërarchisch ondergeschikte, zoals een werknemer,[37] geen geldige verwerkingsgrondslag biedt.[38]

Een ander euvel waar veelvuldig op is gewezen, is dat de richtlijn geen aparte bepaling bevat ten aanzien van kinderen, die juist een groot deel van de gebruikers van internetdiensten als Facebook en Hyves uitmaken. In de verordening is een nieuw artikel opgenomen ten aanzien van kinderen,[39] waarin onder meer is bepaald dat in geval van het rechtstreeks aanbieden van internetdiensten aan kinderen jonger dan 13 jaar, de verwerking van persoonsgegevens slechts rechtmatig is wanneer en voor zover de ouder of voogd van het kind daartoe toestemming heeft gegeven. Ook dient de verantwoordelijke dat wat redelijkerwijs van hem kan worden verwacht te doen om verifieerbare toestemming te verkrijgen.[40] Ook andere artikelen in de verordening bieden kinderen extra bescherming. Daarnaast zijn de plichten van de verantwoordelijke onder de verordening uitgebreid. Zo dient hij uitgebreide documentatie bij te houden van de door hem uitgevoerde verwerking van persoonsgegevens,[41] dient hij verdere maatregelen te treffen om de gegevens adequaat te beveiligen,[42] dient hij privacyeffectbeoordelingen of -assessments uit te voeren[43] en dienen grotere bedrijven verplicht een functionaris voor de gegevensbescherming aan te stellen.[44]

De grootse veranderingen zijn echter doorgevoerd op het gebied van de regulering en de handhaving van de in de verordening vervatte rechten en plichten. Ten eerste moet worden opgemerkt dat het hier een verordening betreft, geen richtlijn, wat met zich meebrengt dat de soms nogal diverse nationale regels worden geharmoniseerd en gestandaardiseerd, aangezien een verordening directe werking heeft. Daarbij is de Europese Commissie bevoegd verdere invulling te geven aan de bepalingen[45] en krijgt de Artikel 29-werkgroep een prominentere rol.[46] Daarnaast is er gekozen voor een zogenoemd 'one-stop-shop'-systeem, waarbij het mogelijk wordt dat niet elke 'CBP' in zijn eigen rechtsgebied de dataprotectieregels handhaaft, maar er één regulator kan worden aangewezen die één bedrijf of een specifieke verwerking in geheel Europa beoordeelt en reguleert.[47] Ook is de boetebevoegdheid van deze instanties enorm gegroeid, wat noodzake-

29. Zie o.a. www.cbpweb.nl/Pages/ind_wetten_zelfr_gedr.aspx.
30. Artikel 18 Dataprotectierichtlijn.
31. Artikel 29-30 Dataprotectierichtlijn.
32. Ook is de lijst met definities aanzienlijk gegroeid. Artikel 4 Algemene verordening gegevensbescherming.
33. Zie ook: P.H. Blok, 'De waarde van de omnibuswet', *P&I* 2005-6.
34. Artikel 2 onder h Dataprotectierichtlijn. Zie ook: Artikel 29-werkgroep, *Opinion 04/2012 on Cookie Consent Exemption*, 00879/12/EN, WP 194, Brussel, 7 juni 2012.
35. Artikel 4 onder 8 Algemene verordening gegevensbescherming.
36. J.M. Titulaer-Meddens, 'De Algemene verordening gegevensbescherming en het bedrijfsleven', *P&I* 2012-3, p. 102.
37. Overweging 34 Algemene verordening gegevensbescherming.
38. Artikel 7 Algemene verordening gegevensbescherming.
39. Een kind is een persoon jonger dan 18 jaar. Artikel 4 onder 18 Algemene verordening gegevensbescherming.
40. Artikel 8 Algemene verordening gegevensbescherming.
41. Artikel 28 Algemene verordening gegevensbescherming.
42. Artikel 30 Algemene verordening gegevensbescherming.
43. Artikel 33 Algemene verordening gegevensbescherming.
44. Artikel 35 Algemene verordening gegevensbescherming. Zie verder: artikel 36-37 Algemene verordening gegevensbescherming.
45. Artikel 86-87 Algemene verordening gegevensbescherming en verder in de specifieke artikelen, zoals ook bij het recht om vergeten te worden, artikel 17 lid 9, het recht op dataportabiliteit, artikel 18 lid 3, en het recht ten aanzien van profilering, artikel 20 lid 5.
46. De werkgroep zal hernoemd worden: Europees Comité voor gegevensbescherming. Artikel 64-72 Algemene verordening gegevensbescherming.
47. Artikel 46-54 Algemene verordening gegevensbescherming.

lijk werd geacht om grote multinationals ook daadwerkelijk af te kunnen schrikken. Nu kan in sommige gevallen de toezichthoudende autoriteit een geldboete van een miljoen euro opleggen of, bij een onderneming, een geldboete van 2% van de jaarlijkse wereldwijde omzet.[48]
Tot slot zijn er uitgebreidere regels opgesteld omtrent de reikwijdte en de toepassing van de richtlijn met betrekking tot internationaal gegevensverkeer,[49] dat steeds belangrijker wordt in verband met buitenlandse (internet)bedrijven die actief zijn op de Europese markt, Europese bedrijven met internationale dependances en de opkomende techniek van cloudcomputing.[50]
Daarnaast is er een aantal belangrijke wijzigingen doorgevoerd ten aanzien van de rechten van de consument, ofwel het datasubject. De belangrijkste drie worden achtereenvolgens in de volgende paragrafen toegelicht: het recht om vergeten te worden, het recht op dataportabiliteit en de bescherming tegen profiling. Daarbij zal eerst worden beschreven wat de huidige richtlijn hieromtrent vermeldt, welke problemen er worden gesignaleerd ten aanzien van de huidige regelgeving, wat het nieuwe voorstel in de verordening behelst en tot slot zal worden beoordeeld wat de voor- en nadelen zijn van het nieuwe voorstel.

3. Het recht om vergeten te worden

De huidige richtlijn kent het datasubject het recht toe op de rectificatie, de uitwissing en de afscherming van de gegevens waarvan de verwerking niet overeenstemt met de bepalingen van de richtlijn; het datasubject heeft tevens recht op de kennisgeving aan derden aan wie de gegevens zijn verstrekt, van elke rectificatie, uitwissing of afscherming.[51] Uit de praktijk blijkt echter dat rechthebbenden nauwelijks gebruikmaken van deze rechten. Uit een steekproef in Nederland bleek bijvoorbeeld dat maar liefst 45% van de ondervraagde organisaties nooit een inzageverzoek had ontvangen, dat slechts 22% van de organisaties regelmatig een verzoek tot correctie of aanvulling van gegevens had ontvangen, dat de helft van de organisaties een dergelijk verzoek slechts zelden ontving en dat eenvijfde van de ondervraagde organisaties hier nimmer mee te maken had. 'De zwaardere instrumenten zoals officiële klachten, bezwaar of verzet over privacyaspecten komen maar weinig voor, en ook geschilbeslechtingsprocedures bij de rechter, het CBP en geschillencommissies zijn een zeldzaamheid.'[52]
Daarnaast wordt in toenemende mate betwijfeld of het recht op de rectificatie en de uitwissing van gegevens wel effectief is in de huidige, digitale omgeving. 'What happens on the internet, stays on the internet', is een veel gehoord adagium.[53] Staat een onbezonnen tweet, een naaktfoto of een filmpje met een persoon in beschonken toestand eenmaal op het internet, dan komt het er moeilijk weer af. Doordat het internet het kopiëren, repliceren, downloaden en weer uploaden van materiaal zo eenvoudig maakt, kan bepaalde informatie weliswaar bij de bron worden aangepakt, maar garandeert dit geenszins dat deze niet elders op het internet wordt verspreid. Hierdoor wordt gevreesd dat personen in de toekomst steeds zullen worden geconfronteerd met hun verleden, wat schadelijke gevolgen kan hebben voor hun sociale, persoonlijke en zakelijke ontwikkeling.[54] Vooral met betrekking tot kinderen wordt dit als zeer bezwaarlijk gezien nu het gevaar dreigt dat kinderen door de constante herinnering aan hun verleden worden gehinderd in deze ontwikkeling of, in reactie op dit gevaar, worden geremd in hun experimenteerdrift.
Er gaan dan ook steeds meer stemmen op om het recht op rectificatie en verzet uit te breiden en te herzien; zo is er veel discussie ontstaan over de (on)mogelijkheid voor datasubjecten of hun erven om een facebookpagina op te heffen, bijvoorbeeld na de dood van het datasubject. Interessant in dit verband is het onlangs door het Europees Hof voor de Rechten van de Mens (EHRM) gewezen arrest van *Mosely/VK* waarin centraal stond een filmpje gemaakt van Max Mosely, voorzitter van de Fédération Internationale de l'Automobile (FIA) en zoon van de voormalig leider van de British Union of Fascists, waarin hij zich door vijf in Duits uniform geklede dames als gevangene liet meevoeren in SM-gerelateerde handelingen. De krant *News of the World* plaatste de video op haar website en vervolgens werden de taferelen binnen twee dagen door 1,4 miljoen mensen bestudeerd en werden de beelden op andere pagina's gekopieerd. De vermogende Mosely vroeg in deze zaak niet om een schadevergoeding, wat hij niet als daadwerkelijke bescherming van zijn recht zag, maar verzocht het EHRM om aan journalisten in gevallen gelijk aan de zijne de plicht op te leggen om de publicatie van tevoren te melden aan het datasubject, die daarop de rechter om een publicatieverbod zou kunnen verzoeken. Het Hof volgt in deze zaak echter de Britse overheid die stelt dat een dergelijke plicht in strijd zou zijn met de vrijheid van meningsuiting en een chilling effect voor journalisten met zich mee zou kunnen brengen.[55]
Alhoewel een dergelijke uitbreiding van het recht op inzage en uitwissing derhalve vooralsnog niet wordt geaccepteerd, bevat de verordening wel een met veel bombarie

48. Artikel 73-79 Algemene verordening gegevensbescherming.
49. Zie over actuele dillema's o.a.: Artikel 29-werkgroep, *Advies 8/2010 over toepasselijk recht*, 0836-2/10/NL, WP 179, Brussel, 16 december 2010.
50. Artikel 40-45 Algemene verordening gegevensbescherming. Zie omtrent actuele dillema's o.a.: Artikel 29-werkgroep, *Opinion 05/2012 on Cloud Computing*, 01037/12/EN, WP 196, Brussel, 1 juli 2012.
51. Artikel 12 Dataprotectierichtlijn.
52. H.B. Winter, P.O. de Jong, A. Sibma, F.W. Visser, M. Herweijer, A.M. Klingenberg & H. Prakken, *Wat niet weet, wat niet deert. Een evaluatieonderzoek naar de werking van de Wet bescherming persoonsgegevens in de praktijk*, Den Haag: WODC, Ministerie van Justitie 2008, p. 82-83; *Kamerstukken II* 2006/07, 31 051 (BLG19029); www.wodc.nl/images/1382b-volledige-tekst_tcm44-165373.pdf. Zie daarover: H.B. Winter, 'De werking van de WBP in kaart gebracht: onbekend maakt onbemind', *RegelMaat* 2009-2; A.M. Klingenberg, 'Wat niet weet, wat niet deert: de evaluatie van de Wet bescherming persoonsgegevens', *P&I* 2009-2.
53. Zie ook: W. Hins, 'Het ijzeren geheugen van internet', *AA* juli/augustus 2008.
54. Zie ook: L. Costa & Y. Poullet, 'Privacy and the regulation of 2012', *Computer Law & Security Review* 2012-28, p. 257.
55. EHRM 10 May 2011, Application no. 48009/08 (*Mosley/The United Kingdom*);),W. Hins, 'Annotatie bij EHRM 10 mei 2011 (Mosley/Verenigd Koninkrijk)', *European Human Rights Cases* 2011-108.

aangekondigd recht om vergeten te worden;[56] dat recht is afgeleid van het uit het Franse strafrecht afkomstige 'droit de oblier',[57] dat misdadigers garandeert dat zij, nadat zij hun straf hebben uitgezeten, bij herintreding in de maatschappij hun leven met een schone lij kunnen beginnen.[58] Het voorstel uit de verordening stelt dat het datasubject er recht op heeft dat de voor de verwerking verantwoordelijke ervoor zorgdraagt dat hem betreffende gegevens worden gewist en de verdere verspreiding van dergelijke gegevens achterwege blijft, met name waar het gaat om persoonsgegevens die door de betrokkene als kind beschikbaar zijn gesteld. Dit recht heeft het datasubject wanneer de gegevens niet langer nodig zijn voor het doel waarvoor zij werden verwerkt, hij zijn aanvankelijke toestemming voor de verwerking intrekt, als hij bezwaar heeft gemaakt tegen de verwerking of als de gegevensverwerking onrechtmatig is.[59] Belangrijk is dat wanneer de verantwoordelijke de persoonsgegevens openbaar heeft gemaakt, bijvoorbeeld door ze op internet te publiceren, hij alle (technische) maatregelen dient te treffen om anderen die deze gegevens hebben gekopieerd, gedownload of anderszins hebben verwerkt ervan op de hoogte te stellen dat het datasubject om de verwijdering van zijn gegevens heeft verzocht.[60] Er staan echter ook een aantal zeer belangrijke uitzonderingen op dit recht vermeld,[61] waarvan de belangrijkste is het geval waarin er een conflict bestaat met de uitingsvrijheid,[62] waaraan doorgaans het recht op toegang tot informatie wordt gekoppeld. Daarenboven hoeft de verantwoordelijke de verwerking van de gegevens slechts te beperken, in plaats van ze te wissen,[63] onder andere als de juistheid ervan door de betrokkene wordt betwist, gedurende een periode die de verantwoordelijke in staat stelt de juistheid van de gegevens te controleren.

In de wetenschappelijke literatuur en daarbuiten is veel kritiek ontstaan omtrent dit voorstel.[64] De meest fundamentele kritiek komt, zoals bij de zaak *Mosely*, vanuit de vrijheid-van-meningsuitingshoek.[65] Alhoewel op het recht om vergeten te worden een uitzondering wordt gemaakt in het geval van een botsing met het recht op de vrijheid van meningsuiting, vrezen zij dat de introductie van dit recht tot censuur kan leiden, het publieke debat kan perverteren doordat bepaalde berichten of informatie die daarvan onderdeel vormen worden verwijderd, wijzen zij erop dat dit recht kan leiden tot een chilling effect bij internetdiscussiefora en prijzen zij juist de archieffunctie van het internet en de historische en culturele waarde daarvan.[66] Aangenomen wordt dat dit recht niet alleen betrekking heeft op berichten en informatie die een persoon over zichzelf heeft gepost, maar ook op berichten die anderen hebben gepubliceerd over deze persoon, wat grote gevolgen voor hun rechten zou kunnen hebben.[67] Daarnaast worden er praktische bezwaren geopperd aangezien onduidelijk is welke mate van zorg de verantwoordelijke dient te betrachten, wat kan leiden tot rechtsonzekerheid.[68]

Aan de andere kant wordt er juist op gewezen dat dit recht, dat aanvankelijk een veel grotere en absolutere reikwijdte leek te krijgen, thans zeer is afgezwakt en er zeer grote uitzonderingen op bestaan, zodat het slechts een marginale aanvulling is ten aanzien van het in de richtlijn opgenomen recht op bezwaar en rectificatie.[69] Vrijwel iedere publicatie en informatieverstrekking heeft immers een relatie tot de uitingsvrijheid. Het is dan ook onduidelijk in hoeverre het recht om vergeten te worden een uitbreiding betekent van het recht op inzage, rectificatie en uitwissing. Al met al is het zeer de vraag of dit artikel in deze vorm ook in de definitieve versie van de verordening zal worden opgenomen.

4. Het recht op dataportabiliteit

Er woedt al lange tijd een discussie omtrent de positie en de handelwijzen van internetdiensten als Facebook en Google. Daarbij worden met name twee bezwaren herhaaldelijk te berde gebracht. Ten eerste wordt er gewezen op de steeds dominanter wordende positie van deze bedrijven, die alleen maar groter lijkt te gaan worden. Ten tweede is het businessmodel van dergelijke bedrijven gericht op het verzamelen van persoonsgegevens, het opstellen van persoons- of groepsprofielen en het op basis daarvan aanbieden van persoonsgerichte reclame. Deze persoonsgebonden reclames zijn effectiever dan generieke reclames, een modefetisjist zal zich immers eerder laten

56. Zie ook: I. Szekely, 'The right to forget, the right to be forgotten: Personal Reflections on the fate of personal data in the information society', in: S. Gutwirth, R. Leenes, P. De Hert & Y. Poullet, *European Data Protection: In Good Health?*, Dordrecht: Springer 2012.
57. Als voorloper van dit voorstel wordt gezien het verzoek van het Spaanse CBP uit 2011, waarmee het Google verzocht links te verwijderen naar onlinenieuwsberichten aangezien deze achterhaalde informatie zouden bevatten en derhalve de privacy van Spaanse burgers zouden beknotten.
58. Zie ook: V. Mayer-Schönberg, *Delete: The virtue of forgetting in the digital age*, Princeton: Princeton University Press 2009.
59. Artikel 17 lid 1 Algemene verordening gegevensbescherming.
60. Artikel 17 lid 2 Algemene verordening gegevensbescherming. Dit is afgezwakt ten aanzien van een eerdere versie van dit artikel waarin was vermeld: 'Where the controller referred to in paragraph 1 has made the data public, it shall in particular ensure the erasure of any public Internet link to, copy of, or replication of the personal data relating to the datasubject contained in any publicly available communication service which allows or facilitates the search of or access to this personal data.'
61. Artikel 17 lid 3 Algemene verordening gegevensbescherming.
62. Zie ook: artikel 80 Algemene verordening gegevensbescherming.
63. Artikel 17 lid 4 Algemene verordening gegevensbescherming. Lid 5 tot en met 8 blijven hier verder onbesproken.
64. Zie o.a. S.C. Bennett, 'The "Right to be Forgotten": Reconciling EU and US Perceptives', *Berkeley Journal of International Law* 2012-30; K. Eltis, 'Breaking through the "Tower of Babel": a "right to be forgotten" and how trans-systemic thinking can help reconceptualize privacy harm in the age of analytics', *Fordham Intellectual Property, Media & Entertainment Law Journal* 2011-22.
65. J. van Hoboken, 'Het recht op vergetelheid: een oud recht in een verkeerd jasje', *P&I* 2012-3. Zie ook: www.jorisvanhoboken.nl/?p=308.
66. Zie verder: R.H. Weber, 'The Right to be Forgotten: More than a Pandora's Box?', *JIPITec* 2011-2.
67. J. Rosen, 'The Right to be Forgotten', *Stanford Law Review Online* 2012-64. Zie ook: http://peterfleischer.blogspot.nl/2011/03/foggy-thinking-about-right-to-oblivion.html.
68. J. Ausloos, 'The "Right to be Forgotten" – Worth remembering?', *Computer Law & Security Review* 2012-28.
69. www.aidh.org/Actualite/Act_2010/Images/Charte_oubli_La_Charte.pdf; www.statewatch.org/news/2011/dec/eu-com-draft-dp-reg-inter-service-consultation.pdf.

verleiden door de nieuwe collectie van Zara dan door afgeprijsde Zeemanshirtjes, en vertegenwoordigen daarom een hogere waarde. Aangezien veel internetdiensten gratis te gebruiken zijn, maar er in ruil daarvoor wel persoonsgegevens worden verwerkt (gevraagd of ongevraagd), worden persoonsgegevens in toenemende mate gezien als het digitale betaalmiddel.[70] Omdat persoonsgegevens de belangrijkste of, zoals bij Facebook, zelfs enige 'asset' is van deze bedrijven zijn zij er zeer op gebrand hierover controle te houden.

Het voorstel van de verordening lijkt deze bezwaren te willen ondervangen door de introductie van een zogenoemd recht op dataportabiliteit.[71] Dit is geënt op het reeds bestaande recht op nummerportabiliteit,[72] waarmee onder meer wordt gegarandeerd dat alle abonnees die daarom verzoeken hun telefoonnummers kunnen behouden en dat hier geen exorbitante kosten voor in rekening mogen worden gebracht. Deze nummers moeten bovendien zo snel mogelijk worden overgedragen en geactiveerd.[73] Nummerportabiliteit bevordert op deze wijze de keuzevrijheid van de consument en de daadwerkelijke mededinging op de concurrerende markten voor elektronische communicatie.[74]

In de verordening wordt door middel van de introductie van een recht op dataportabiliteit ditzelfde principe toegepast op persoonsgegevens die in het bezit zijn van een verantwoordelijke en tracht daarmee tevens de positie van de consument te versterken en de concurrentie in de markt voor persoonsgegevens te vergroten. Ten eerste garandeert het dat wanneer persoonsgegevens elektronisch en in een gestructureerd en algemeen gebruikt format worden verwerkt, het datasubject recht heeft op een kopie van de gegevens, die het vervolgens verder mag gebruiken naar eigen inzicht.[75] Ten tweede is bepaald dat als de verwerking van persoonsgegevens wordt verwerkt op basis van de toestemming van het datasubject of een overeenkomst, zoals bij bijvoorbeeld Facebook het geval is, het datasubject het recht heeft om deze persoonsgegevens en alle andere informatie die hij heeft verstrekt en die is bewaard, in een algemeen gebruikt elektronisch format over te dragen naar een ander geautomatiseerd verwerkingssysteem.[76] Zo kan een facebookgebruiker zijn profiel meenemen naar een ander sociaal netwerk en krijgt hij meer controle over zijn eigen gegevens.[77]

Het recht wordt over het algemeen positief onthaald in de literatuur,[78] mede omdat het bijdraagt aan systeemoperabiliteit.[79] Het recht wordt ook gezien als belangrijk hulpmiddel om mensen weer controle te geven over hun data, de macht van bepaalde bedrijven te doorbreken en lock-ineffecten te voorkomen. Toch wordt erop een aantal problemen gewezen. Alhoewel het recht met name is bedoeld voor sociale netwerken en de relatie tussen klanten en internetproviders,[80] kan het recht ook gevolgen hebben voor andere verwerkers van persoonsgegevens, wat grote administratieve lasten met zich mee kan brengen. Daarnaast bestaat er discussie over de vraag hoe effectief en relevant voor de praktijk het recht is nu het datasubject wel zijn eigen gegevens kan meenemen naar een ander sociaal netwerk, maar niet die van zijn vrienden.[81] De vraag is daarnaast of een dergelijk overzetten van data geen nadelige effecten zal hebben voor (bevriende) derden, doordat het deel van hun profiel dat is gekoppeld aan dat van hem kan wegvallen of niet meer wordt geüpdatet.[82] Tot slot wordt er op gewezen dat deze bepaling, die zo duidelijk doelt op het huidige internetlandschap, de sociale media en dan met name Facebook, erg techniekafhankelijk is en daarmee het gevaar loopt snel achterhaald te zijn en bepaalde diensten wel en andere diensten niet te reguleren. '[L]egislating in a constantly evolving field risks making the law seem outdated and irrelevant. New regulations, that could perhaps be interpreted as favouring one over another competing internet platforms, could also decidedly affect (or even distort) a process in the making that could ultimately change the internet as we know it – admittedly, not a task of data protection legislators.'[83]

70. M. Kuneva (then Commissioner for Consumer Protection), *European Consumer Commissioner, Keynote Speech*, p. 2, Roundtable on Online Data collection, targeting and profiling, Brussel, 31 maart 2009.
71. Zie verder: S. Weiss, 'Privacy threat model for data portability in social network applications', *International Journal of Information Management* 2009-29; U. Bojars, A. Passant, J.G. Breslin & S. Decker, 'Social Network and Data Portability using Semantic Web Technologies', http://ceur-ws.org/Vol-333/saw1.pdf.
72. Zie ook: Overweging 40-42 Universeledienstrichtlijn. Richtlijn 2002/22/EG van het Europees Parlement en de Raad van 7 maart 2002 inzake de universele dienst en gebruikersrechten met betrekking tot elektronische-communicatienetwerken en -diensten (Universeledienstrichtlijn).
73. Artikel 30 Universeledienstrichtlijn.
74. Overweging 47 Richtlijn Burgerrechten. Richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009 tot wijziging van Richtlijn 2002/22/EG inzake de universele dienst en gebruikersrechten met betrekking tot elektronischecommunicatienetwerken en -diensten, Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie en Verordening (EG) nr. 2006/2004 betreffende samenwerking tussen de nationale instanties die verantwoordelijk zijn voor handhaving van de wetgeving inzake consumentenbescherming (Richtlijn Burgerrechten).
75. Artikel 18 lid 1 Algemene verordening gegevensbescherming.
76. Artikel 18 lid 2 Algemene verordening gegevensbescherming.
77. Zie ook: Overweging 55 Algemene verordening gegevensbescherming.
78. F. Gilbert, 'EU Data Protection Overhaul: New Draft Regulation', *The Computer & Internet Lawyer* 2012-3, p. 3.
79. P. De Hert & V. Papakonstantinou, 'The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals', *Computer Law & Security Review* 2012-28, p. 137-138.
80. H. Hijmans, 'Nieuwe Europese regels voor privacy: commissie stelt pakket voor om gegevens ook in het informatietijdperk te beschermen', *NTER* 2012-4, p. 137.
81. G. Hornung, 'A General Data Protection Regulation for Europe? Light and Shade in the Commissions Draft of 25 January 2012', *Scipted* 2012-1, p. 74.
82. L. Costa & Y. Poullet, p. 257.
83. P. De Hert & V. Papakonstantinou, p. 137-138.

5. Profiling

We leven in een 'profiled world', zo luidt een veelgehoord credo.[84] Profielen worden niet alleen gebruikt voor het aanbieden van advertenties, maar ook om nieuws op sites te personaliseren, door staten om criminelen en terroristen op te sporen en om beslissingen te maken ten aanzien van personen, zoals het toekennen van een lening door een bank of een verzekering door een zorgverzekeraar. De gevaren die dit proces met zich mee kan brengen zijn globaal in twee groepen in te delen. Ten eerste is er gevaar van discriminatie en stigmatisatie, doordat bepaalde groepen met bijvoorbeeld een etnische of sociale achtergrond worden uitgesloten van bepaalde mogelijkheden of een speciale behandeling worden aangemeten. Dit kan geschieden op basis van etnische of sociale persoonsgegevens, maar kan ook plaatshebben door middel van verhullende gegevens; dit wordt 'redlining' genoemd. Een bekend voorbeeld hiervan is dat voorheen sommige Amerikaanse banken leningen weigerden niet op basis van raciale kenmerken, maar op basis van postcodes die evenwel zeer raciaal waren gedetermineerd.[85] Ten tweede zijn er dataprotectieproblemen en het daaraan verbonden gevaar van de-individualisering, doordat er op grote schaal persoonsgegevens worden verzameld en gebruikt en doordat niet een persoon en zijn persoonlijke omstandigheden centraal komen te staan in de besluitvorming, maar algemene groepskenmerken en statistische verbanden, zoals de relatie tussen mensen die viltjes onder hun meubelen plaatsen en zij die hun lening op tijd afbetalen.[86]

Naast de algemene regels omtrent dataminimalisatie en de eisen omtrent correcte en nauwkeurige gegevensverwerking die ook ten aanzien van profiling gelden,[87] kent de richtlijn eenieder het recht toe '[…] niet te worden onderworpen aan een besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem in aanmerkelijke mate treft en dat louter wordt genomen op grond van een geautomatiseerde gegevensverwerking die bestemd is om bepaalde aspecten van zijn persoonlijkheid, zoals beroepsprestatie, kredietwaardigheid, betrouwbaarheid, gedrag, enz. te evalueren.'[88] Desalniettemin kan een persoon toch aan een dergelijk besluit worden onderworpen, bijvoorbeeld het weigeren van een hypothecaire lening door een bank op basis van een profiel, indien dat besluit wordt genomen in het kader van het sluiten of uitvoeren van een overeenkomst, mits aan het verzoek van de betrokkene is voldaan of passende maatregelen, zoals de mogelijkheid zijn standpunt te doen gelden, zijn genomen ter bescherming van zijn gerechtvaardigde belang, of als het besluit zijn grondslag vindt in een wet waarin de maatregelen zijn omschreven die strekken tot bescherming van het gerechtvaardigde belang van het datasubject.[89] Elk datasubject heeft daarnaast het recht op de mededeling van de logica die ten grondslag ligt aan de automatische besluitvorming.[90]

In de literatuur wordt erop gewezen dat dit artikel, dat werd geschreven toen de schaal en omvang die profiling thans aanneemt nog niet of nauwelijks was te voorspellen, nodig aan vervanging toe is. Zo wordt de formulering over het algemeen gezien als vaag. Wat bijvoorbeeld precies een 'besluit' inhoudt, hoe zich dit onderscheidt van andere plannen, adviezen en voornemens en of een besluit, dat een mentale beslissing lijkt te suggereren, ook aanwezig is bij een geheel of gedeeltelijke genomen computerbeslissing blijft onduidelijk. Onduidelijkheid bestaat tevens ten aanzien van de vraag hoe groot of belangrijk de rechtsgevolgen of de aanmerkelijke mate waarin een besluit een persoon treft moeten zijn. Daarbij wordt erop gewezen dat het artikel eenvoudig omzeild kan worden door de besluitvorming niet *louter* geautomatiseerd te doen laten plaatshebben. Ook moet de beslissing betrekking hebben op bepaalde aspecten van iemands persoonlijkheid, waarbij een niet-limitatieve opsomming wordt gegeven, waardoor het onduidelijk blijft welke andere gevallen hier precies onder vallen.[91]

Problematisch is dat er zeer weinig jurisprudentie is ten aanzien van dit artikel, zodat deze onduidelijkheden geen verdere invulling hebben gekregen. Tot slot wordt erop gewezen dat de uitzonderingen op dit recht zeer groot zijn, dat het hier een recht van het datasubject betreft waarop hij indien hij dat wenselijk acht een beroep kan doen, geen te allen tijde in acht te nemen gebod waarmee de verantwoordelijke rekening dient te houden en dat het voor veel mensen überhaupt onduidelijk is dat zij

84. Zie o.a.: D. Skillicorn, *Knowledge Discovery for Counterterrorism and Law Enforcement*, Boca Raton: Taylor & Francis Group, LLC 2009; D.T. Larose, *Data mining methods and models*, New Yersey: John Wiley & Sons, Inc. All. 2006; M. Hildebrandt & S. Gutwirth (red.), *Profiling the European Citizen Cross-Disciplinary Perspectives*, New York: Springer 2008; C. Westphal, *Data mining for Intelligence, Fraud & Criminal Detection*, Boca Raton: Taylor & Francis Group, LLC 2009.
85. Zie o.a. J. Beuving, J.W. Heuver & W. van Helden, 'Etniciteit, profilering en het gelijkheidsbeginsel', *NJB* 2006, 34; K. Guzik, 'Discrimination by Design: Data Mining in the United States's "War on Terrorism", *Surveillance & Society* 2009-7; P. Kuhn, 'Sex discrimination in labor markets: The role of statistical evidence', *The American Economic Review* 1987-77; M. LaCour-Little, 'Discrimination in mortgage lending: A critical review of the literature', *Journal of Real Estate Literature* 1999-7; G.D. Squires, 'Racial profiling, insurance style: Insurance redlining and the uneven development of metropolitan areas', *Journal of Urban Affairs* 2003-25.
86. Zie o.a. B.W. Schermer, 'The limits of privacy in automated profiling and data mining', *Computer Law & Security Review* 2011-27; A. Roosendaal Vind ik dit leuk? Een fundamenteel privacyperspectief op monitoring en profilingtechnologieën', *P&I* 2011-3; J.S. Fulda, 'Data Mining and Privacy', *Alb. L.J. Sci. & Tech*. 2000-11; V.C. Müller, 'Would you mind being watched by machines? Privacy concerns in data mining', *AI & Soc* 2009-23; T.Z. Zarsky, 'Mine your own business!: making the case for the implications of the data mining of personal information in the forum of public opinion', *Yale Journal of Law & Technology* 2003-5; A. Ramasastry, 'Lost in translation? Data mining, national security and the "adverse inference" problem', *Santa Clara Computer & High Tech. L.J.* 2006-22; W.N. Renke, 'Who controls the past now controls the future: counter-terrorism, data mining and privacy', *Alta. L. Rev*. 2006-43; B.W. Schermer, 'The limits of privacy in automated profiling and data mining', *Computer Law & Security Review* 2011-7; H.T. Tavani, 'Genomic research and data-mining technology: Implications for personal privacy and informed consent', *Ethics and Information Technology* 2004-6.
87. Zie ook: E. Hoving, 'Modellering van persoonsgegevens en groepsprofielen', *P&I* 2008-6.
88. Artikel 15 lid 1 Dataprotectierichtlijn. Zie hierover ook: W. Schreurs, 'Ik ben user 712. Recht op toegang tot persoonsgegevens en op mededeling van de logica van geautomatiseerde verwerking', *Computerrecht* 2009-40.
89. Artikel 15 lid 2 Dataprotectierichtlijn.
90. Artikel 12 Dataprotectierichtlijn.
91. L.A. Bygrave, 'Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling', *Computer Law & Security Report* 2001-17.

onderworpen zijn aan geautomatiseerde besluitvorming, waardoor het belang van recht om hier inzage in te krijgen of tegen op te komen wordt gemarginaliseerd.[92]

Onder de verordening is het artikel omtrent profiling herzien.[93] Lid 1 van het artikel stelt dat iedere natuurlijke persoon het recht heeft niet te worden onderworpen aan een maatregel waaraan voor hem rechtsgevolgen zijn verbonden of die hem in aanmerkelijke mate treft en die louter wordt genomen op grond van een geautomatiseerde verwerking die bestemd is om bepaalde aspecten van zijn persoonlijkheid te evalueren of om met name zijn beroepsprestaties, economische situatie, verblijfplaats, gezondheid, persoonlijke voorkeuren, betrouwbaarheid of gedrag te analyseren of te voorspellen. Daarbij vermeldt lid 3 dat de geautomatiseerde gegevensverwerking die bestemd is om bepaalde aspecten van de persoonlijkheid van een natuurlijke persoon te beoordelen, niet uitsluitend gebaseerd mag worden op bijzondere persoonsgegevens.[94] Lid 2 bevat wederom een aantal uitzonderingen op dit recht en stelt dat een persoon *alleen* aan een maatregel als bedoeld in lid 1 mag worden onderworpen in drie gevallen. Ten eerste wanneer de verwerking wordt uitgevoerd in het kader van het sluiten of het uitvoeren van een overeenkomst en aan het door de betrokkene ingediende verzoek tot het sluiten of het uitvoeren van de overeenkomst is voldaan of passende maatregelen zijn aangeboden ter bescherming van de gerechtvaardigde belangen van de betrokkene, zoals het recht op menselijke tussenkomst. Ten tweede is er een uitzondering wanneer de verwerking uitdrukkelijk is toegestaan op grond van wetgeving en ten derde wanneer de verwerking plaatsvindt op grond van de toestemming van de betrokkene. Wat opvalt is dat het artikel niet fundamenteel is gewijzigd, maar dat het in grote lijnen overeenstemt met het oorspronkelijke artikel, waardoor veel van de gesignaleerde problemen niet worden ondervangen,[95] de bepaling nog steeds als vaag en onpraktisch wordt ervaren[96] en er wederom een roep klinkt om meer duidelijkheid.[97] Daarbij wordt er in de nieuwe bepaling nog een extra uitzonderingsgrond gecreëerd in lid 2, namelijk ingeval de verwerking plaatsheeft op basis van de toestemming van het datasubject. Gezien de verzwaarde eisen omtrent toestemming in de verordening lijkt dit evenwel praktisch gezien geen ruime uitzonderingsgrond. Tot slot wordt er door velen op gewezen dat wellicht niet (slechts) voor een juridische oplossing dient te worden gekozen, maar (tevens) voor een technische oplossing, zoals door het inbedden van de dataminimalisatieregels in de technische infrastructuur van dataverwerkingssystemen[98] of het op technische wijze controleren van de toepassing en het gebruik van de persoonsprofielen in de praktijk op discriminatie- en privacyproblemen.[99]

Toch wordt het nieuwe artikel over het algemeen positief onthaald.[100] Er wordt onder meer op gewezen dat er extra bescherming wordt geboden door het feit dat lid 2 thans formuleert dat een dergelijk besluit 'alleen' mag worden genomen in de daarin opgesomde gevallen, wat met zich meebrengt dat het in tegenstelling tot het recht in de richtlijn een gebod betreft dat geldt ook al heeft het datasubject er geen beroep op gedaan. Tot slot biedt ook de nieuw toegevoegde uitzondering met betrekking tot de geautomatiseerde besluitvorming die slechts op basis van bijzondere persoonsgegevens geschiedt extra bescherming ten opzichte van de richtlijn. Toch is het de vraag of deze gewijzigde bepaling zo afdoende bescherming biedt tegen de gevaren van profiling in een wereld waarin deze techniek steeds wijder verbreid raakt.

6. Analyse: recht, plicht of deugd

Zo rond de jaren 70 van de 20e eeuw zijn in de Verenigde Staten de zogenoemde Fair Information Practices (FIPs) ontstaan.[101] Deze werden ontwikkeld tegen de achtergrond van de snel opkomende informatietechnieken en dataverwerkingssystemen. Privacy was al langer een recht van de burger om zich te beschermen tegen arbitrair overheidsoptreden en -intreden in de persoonlijke levenssfeer; nu kwamen echter veel van de technische middelen in handen van burgers en bedrijven,[102] die middels camera's, telefoons en computers op grote schaal persoonsgegevens konden verzamelen, doorgeven, opslaan en verwerken. Om dit proces van waarborgen te voorzien werden

92. M. Hildebrandt, 'Who is Profiling Who? Invisible Visibility', p. 248, in: S. Gutwirth, Y. Poullet, P. de Hert, C. de Terwagne & S. Nouwt, *Reinventing Data Protection?*, Brussel: Springer 2009.
93. Zie eerder reeds: Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling (Adopted by the Committee of Ministers on 23 November 2010 at the 1099th meeting of the Ministers' Deputies).
94. Het oorspronkelijke voorstel bevatte nog het volgende lid: Paragraph 2 shall not apply where the processing concerns a child.
95. M. Hildebrandt, 'The Dawn of a Critical Transparency Right for the Profiling Era', *Digital Enlightenment Yearbook* 2012.
96. Zie bijvoorbeeld: C. Kuner, 'The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law', *Privacy & Security Law Report* 2 juni 2012, p. 6-7.
97. Artikel 29-werkgroep, *Advies 01/2012 over de voorstellen voor hervorming van het gegevensbeschermingskader*, 00530/12/NL, WP 191, Brussel, 23 maart 2012, p. 16. Zie ook: EDPS, *Opinion of the European Data Protection Supervisor on the data protection reform package*, Brussel, 7 maart 2012.
98. S. Bu, *Preservation of Patterns and Input-Output Privacy', Proceedings of ICDE*, 2007; T. Calders & S. Verwer, 'Three Naive Bayes Approaches for Discrimination-Free Classification', *Data Mining and Knowledge Discovery* 2010-2; A. Evfimievski, R. Srikant, R. Agrawal & J. Gehrke, *Privacy preserving mining of association rules*, Proceedings of the 8th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2002; D. Pedreschi, S. Ruggieri & F. Turini, 'Discrimination-aware Data Mining', *KDD* 2008; S. Ruggieri, D. Pedreschi & F. Turini, 'Data Mining for Discrimination Discovery', *Transactions on Knowledge Discovery from Data* 2010-4.
99. V.S. Verykios et al., 'State-of-the-art in Privacy Preserving Data Mining', *Sigmod Record* 2004-33; T. Wang & L. Liu, 'Output Privacy in Data Mining', *Transactions on Database Systems* 2011-36; C.C. Porter, 'De-Identified Data and Third Party Data Mining: The Risk of Re-Identification of Personal Information', *Shidler i.L. Com. & Tech.* 2008-30; M. Kantarcioglu, J. Jin & C. Clifton, 'When do data mining results violate privacy?', Proceedings of the 10th ACM SIGKDD International Conference on Knowledge Discovery and Data mining, New York: ACM 2004.
100. L. Costa & Y. Poullet, p. 258-259.
101. Zie o.a.: http://aspe.hhs.gov/DATACNCL/1973privacy/tocprefacemembers.htm; http://epic.org/privacy/ppsc1977report/.
102. Zie ook: L.D. Warren & S.D. Brandeis, 'The Right to Privacy', *Harvard Law Review* 1980-5.

de FIPs geïntroduceerd, die inzetten op redelijke en zorgvuldige gegevensverwerking.

Deze FIPs hadden een grote invloed op de Europese Dataprotectierichtlijn uit 1995. Net zoals de FIPs, zet de Dataprotectierichtlijn niet primair in op restricties, verboden en beperkingen, maar voornamelijk op zorgvuldigheidsprincipes, belangenafwegingen en transparantie. Het inzetten op dergelijke zorgplichten heeft als belangrijke achterliggende reden dat het dataprotectierecht, in tegenstelling tot het recht op privacy, niet eerst en vooral ziet op de relatie tussen staat en burger, waarbij restricties op overheidshandelen een essentieel onderdeel vormen van de grondrechten van de burger en de grondplichten van de staat, maar tussen burgers en bedrijven onderling. In private relaties geldt als principieel uitgangspunt de vrijheid van handelen en de contractsvrijheid. Daarnaast is de oorsprong van het dataprotectierecht gelegen in de technische ontwikkelingen. Technische ontwikkelingen volgen elkaar snel op zodat de wettelijke bepalingen snel achterhaald kunnen raken, de technieken kunnen eenvoudig zo worden aangepast dat een specifieke formulering of bepaling wordt omzeild en bovendien zijn algemene normen minder remmend voor de ontwikkeling van nieuwe technieken. Deze twee achtergronden vormen de reden om voornamelijk in te zetten op algemene zorgvuldigheidsnormen.

Terwijl in Europa aanvankelijk het recht op dataprotectie werd geschaard onder het recht op privacy, bijvoorbeeld onder de jurisprudentie van artikel 8 EVRM, is het geleidelijk aan een steeds meer onderscheiden rol gaan spelen. Deze ontwikkeling begon door de introductie van de Dataprotectierichtlijn,[103] is voortgezet onder meer door de aanname van een 'lex specialis' van deze richtlijn voor de elektronische omgeving[104] en in het Handvest van de Grondrechten van de Europese Unie worden het recht op privacy en op dataprotectie van elkaar gescheiden. In de verordening wordt deze ontkoppeling verder doorgezet. Terwijl de richtlijn in artikel 1 nog verwijst naar de bescherming van de fundamentele rechten en vrijheden van natuurlijke personen, inzonderheid van het recht op persoonlijke levenssfeer of privacy,[105] spreekt de verordening slechts van het dataprotectierecht en bepalingen in verband met de verwerking van persoonsgegevens. Terwijl de richtlijn 13 keer refereert aan het recht op privacy, doet de verordening dat slechts twee keer.[106] Hiermee lijken het recht op privacy en het recht op dataprotectie definitief van elkaar te worden gescheiden. Dit ligt ook in de lijn der verwachting aangezien één van de belangrijkste redenen om de richtlijn te vervangen was in te spelen op de nieuwe technische ontwikkelingen en de groeiende mogelijkheden van burgers en bedrijven om gegevens te verwerken.[107]

Toch valt op dat de principes die ooit ten grondslag lagen aan het dataprotectierecht juist worden verlaten. De algemene zorgvuldigheidsnormen worden verruild voor specifieke rechten die zien op concrete technische ontwikkelingen: het recht om vergeten te worden, het recht op dataportabiliteit en het recht op bescherming tegen profiling. Daarnaast wordt de rol van de staat en de handhavingsorganen op forse wijze vergroot. Alhoewel de extra rechten voor de consument over het algemeen positief worden onthaald, rijst tevens de vraag of deze ontwikkeling effectief zal zijn.[108] Ten tweede is de vraag in hoeverre het wenselijk is dat de rol van de staat en de handhavende organisaties wordt vergroot, nu wordt gevreesd dat bedrijven zich in reactie hierop geheimzinniger zullen opstellen, er vraagtekens worden geplaatst bij de onafhankelijkheid van de handhavende organisaties en veel staten, met name in de nasleep van 11 september, niet alom worden geprezen om hun privacyvriendelijke beleid. Daarnaast zijn veel mensen heden ten dage simpelweg graag bereid hun persoonsgegevens in te ruilen voor kortetermijnvoordelen als toegang tot gratis internetdiensten;[109] het kan dan ook als paternalistisch worden ervaren dat de staat nu zo'n grote rol krijgt in het beschermen van de burgers tegen zichzelf. Tot slot is, zoals eerder al naar voren kwam, één van de belangrijkste redenen voor het beperkt belang van de dataprotectieregels heden ten dage gelegen in het feit dat consumenten zich niet beroepen op hun rechten en onwetend zijn over veel van de datastromen; deze onwetendheid en laksheid wordt doorgaans niet vergroot door de verantwoordelijkheid van hen weg te nemen en in overheidshanden te leggen, maar wordt hierdoor juist verkleind. Het is derhalve de vraag of de gekozen oplossing de goede is.

Wellicht ware het raadzamer geweest om niet zozeer in te zetten op een vergroting van consumentenrechten, de dataminimalisatieprincipes en bevoegdheden van de handhavende organisaties, maar juist verdere nadruk te leggen op de zorgvuldigheidsnormen. In een tijdperk waarin op elke hoek van de straat een camera hangt, iedere burger met een telefoontje zijn omgeving kan filmen en deze informatie vervolgens op het internet kan plaatsen en waarin het businessmodel van veel nieuwe bedrijven juist is geënt op het verzamelen en gebruiken van persoonsgegevens, is het de vraag of het realistisch is om hier beperkingen aan op te leggen en of het doenlijk is voor de consument om in deze zee van gegevensverkeer zijn eigen data te identificeren, zijn individuele belangen ten aanzien van de verwerking hard te maken en zijn rechten te beschermen en te verdedigen.

De verdere inzet op zorgvuldigheidsprincipes en gecodificeerde deugden van de voor de verwerking verantwoordelijken ware wellicht heilzamer geweest. Ten eerste hinderen zij de technische ontwikkelingen niet en staan ze ook niet in de weg aan de ruilhandel tussen persoons-

103. Alhoewel ook deze voorgangers kent.
104. Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie.
105. Afhankelijk van de Engelse of de Nederlandse vertaling, artikel 1 lid 1 Dataprotectierichtlijn.
106. Dit betreft de Engelse versie van de Algemene verordening gegevensbescherming. L. Costa & Y. Poullet, p. 262.
107. Zie ook: European Commission, *A comprehensive approach on personal data protection in the European Union*, Brussel, 4 november 2010, COM(2010)609 final.
108. Zie ook: L. Costa & Y. Poullet, p. 255.
109. A. Acquisti & J. Grossklags, *What Can Behavioral Economics Teach Us About Privacy?*, www.heinz.cmu.edu/~acquisti/papers/Acquisti-Grossklags-Chapter-Etrics.pdf.

gegevens en 'gratis' internetdiensten, die door veel consumenten als wenselijk wordt ervaren. Daarnaast is het voordeel dat er, in tegenstelling tot de rechten van de consument, geen individueel belang en een (mogelijke) schending van het recht hoeft te worden aangetoond alvorens in rechte kan worden opgetreden. Het beargumenteren van het individuele belang kan lastig zijn in de grote informatiestromen en het belang moet worden gestaafd met aantoonbare (aanstondse) schade. Zoals de zaak *Mosely* reeds liet zien, is de schade dan reeds aangericht en vaak onherstelbaar; een rechtszaak beginnen richt slechts verdere aandacht op de schending en heeft derhalve vaak een averechts effect. Deugden en zorgplichten hebben als voordeel dat ze de verantwoordelijkheid en bewijslast bij de gegevensverwerker leggen, dat er geen sprake hoeft te zijn van schade bij een specifiek individu, maar slechts van een nalatigheid of onzorgvuldigheid, en dat er al kan worden ingegrepen voordat er concrete schade is ontstaan.[110]

Tot slot wordt erop gewezen dat de tendens van harmonisatie en centralisatie van het dataprotectierecht die zich in de verordening voltrekt tevens onwenselijke gevolgen met zich kan meebrengen. Veel landen hebben bijvoorbeeld een andere visie en houding ten aanzien van het dataprotectierecht en de invulling daarvan in concrete normen. Zo staat de Duitse wetgeving op dit gebied bekend als buitengewoon streng, terwijl het Engelse recht een stuk coulanter is; deze verschillen hebben een historische achtergrond en een beperking van de variatie hieromtrent kan een beperking op de zelfbeschikking van een volk met zich meebrengen. Daarbij komt dat al zou het dataprotectierecht op termijn op Europees niveau worden geregeld, veel andere doctrines die de uitoefening van dit recht beïnvloeden, zoals de eerder gesignaleerde botsing met het recht op vrijheid van meningsuiting, nog steeds op nationaal niveau zijn geregeld. De verschillende wijzen waarop deze doctrines in de verschillende rechtsstelsels zijn geïmplementeerd kunnen derhalve alsnog een diversiteit in de toepassing en reikwijdte van het dataprotectierecht met zich meebrengen. Daarnaast valt op dat het dataprotectierecht het enige fundamentele recht is dat zo gedetailleerd op Europees niveau middels een verordening wordt gereguleerd.[111] Het is de vraag wat de legitimatie is voor dit verschil. Tot slot is de vraag welke afweging er dient plaats te vinden als het dataprotectierecht, dat dan Europees zou zijn geregeld, en het recht op vrijheid van meningsuiting, dat voornamelijk nationaal is geregeld, met elkaar in botsing komen, nu als uitgangspunt heeft te gelden dat het Europese recht voorrang heeft.

De nieuwe verordening vormt kortom een dappere poging om het dataprotectierecht meer handen en voeten te geven en een hogere bescherming te bieden aan consumenten in een snel veranderende informatiemaatschappij. Daarbij wordt ten eerste ingezet op de vergroting van de consumentenrechten, met name door de introductie van het recht om vergeten te worden en het recht op dataportabiliteit en door de vergroting van de bescherming tegen profiling. Deze verandering wordt over het algemeen als welkome aanvulling gezien, alhoewel er bij alle drie de rechten op wordt gewezen dat zij wellicht onvoldoende reikwijdte bezitten en onvoldoende concreet zijn geformuleerd om daadwerkelijke rechtsbescherming te bieden aan de consument. Daarnaast wordt voornamelijk ingezet op een vergroting van de bevoegdheden van de handhavende organisaties. Deze twee ontwikkelingen vormen een breuk met de traditionele uitgangspunten van het dataprotectierecht. De tijd zal uitwijzen of dit de bescherming van persoonsgegevens ten goede zal komen.

110.Zie hierover ook: B. van der Sloot, 'Naar een pathologie van privacyschendingen, of over het doel dat de middelen heiligt, *P&I* 2012-2.
111.H. Hijmans, p. 139.